

---

# Unicenter

## NetMaster Network Management for TCP/IP Implementation Guide (incorporating NetSpy and NetMaster Operations) 1<sup>st</sup> edition

P01- 147



**Computer Associates**  
The Software That Manages eBusiness



This documentation and related computer software program (hereinafter referred to as the "Documentation") is for the end user's informational purposes only and is subject to change or withdrawal by Computer Associates International, Inc. ("CA") at any time.

This documentation may not be copied, transferred, reproduced, disclosed or duplicated, in whole or in part, without the prior written consent of CA. This documentation is proprietary information of CA and protected by the copyright laws of the United States and international treaties.

Notwithstanding the foregoing, licensed users may print a reasonable number of copies of this documentation for their own internal use, provided that all CA copyright notices and legends are affixed to each reproduced copy. Only authorized employees, consultants, or agents of the user who are bound by the confidentiality provisions of the license for the software are permitted to have access to such copies.

This right to print copies is limited to the period during which the license for the product remains in full force and effect. Should the license terminate for any reason, it shall be the user's responsibility to return to CA the reproduced copies or to certify to CA that same have been destroyed.

To the extent permitted by applicable law, CA provides this documentation "as is" without warranty of any kind, including without limitation, any implied warranties of merchantability, fitness for a particular purpose or noninfringement. In no event will CA be liable to the end user or any third party for any loss or damage, direct or indirect, from the use of this documentation, including without limitation, lost profits, business interruption, goodwill, or lost data, even if CA is expressly advised of such loss or damage.

The use of any product referenced in this documentation and this documentation is governed by the end user's applicable license agreement.

The manufacturer of this documentation is Computer Associates International, Inc.

Provided with "Restricted Rights" as set forth in 48 C.F.R. Section 12.212, 48 C.F.R. Sections 52.227-19(c)(1) and (2) or DFARS Section 252.227-7013(c)(1)(ii) or applicable successor provisions.

© 2001 Computer Associates International, Inc.

All trademarks, trade names, service marks, and logos referenced herein belong to their respective companies.

# Contents

## Chapter 1: Preparing Communications Server Systems

Configuring the Communications Server Interface .....	1-2
Task 1 – Updating Your SOLVE SSI Configuration .....	1-2
Task 2 – Authorizing Your Started Task User IDs .....	1-3
Task 3 – Authorizing User Functionality .....	1-5
Task 4 – Enabling Access to SNMP Data .....	1-6
Task 5 – Ensuring That Name Resolution Is Enabled .....	1-7
Enabling Communications Server for Connection Awareness .....	1-8
Task 1 – Generating SMF Records .....	1-8
Task 2 – Implementing the SMF Exit Module .....	1-10
Task 3 – Registering the SMF Exit Module .....	1-10
Task 4 – Checking the MVS Dynamic Exits .....	1-12

## Chapter 2: Preparing TCPaccess Systems

Enabling the TCPaccess Interface .....	2-2
Task 1 – Setting Up the Parameter Datasets .....	2-2
Task 2 – Enabling the TCPaccess Exit and Connection Awareness .....	2-3
Task 3 – Setting Up DNR Members .....	2-6
Task 4 – Enabling Access to SNMP Data .....	2-6
Task 5 – Enabling the NETSTAT Interface .....	2-7

## Chapter 3: Other Implementation Tasks

Enabling the System Command Console Interface .....	3-2
Task 1 – Defining a Subsystem ID .....	3-2
Task 2 – Defining Consoles .....	3-2
Setting Up OSA Support .....	3-3

---

## Chapter 4: Initializing NetMaster for TCP/IP

Initializing NetMaster for TCP/IP for the First Time .....	4-2
Task 1 – Logging On .....	4-2
Task 2 – Performing Initial Customization .....	4-2
Task 3 – Reviewing Additional Parameter Groups .....	4-8
Task 4 – Express Setup .....	4-8
Task 5 – Setting up the System Image to Load on Restart .....	4-10
Task 6 – Changing User to Administrator .....	4-11
Dealing with Initialization Failures .....	4-12
Using the System Initialization In Progress Dialog .....	4-12
Where to Next? .....	4-13

# Preparing Communications Server Systems

---

This chapter describes how to prepare Communications Server so that it can work effectively with NetMaster for TCP/IP.

**This chapter contains the following topics:**

- Configuring the Communications Server Interface
- Enabling Communications Server for Connection Awareness

***Important:** Some of the tasks in this chapter require high authority levels.*

## Configuring the Communications Server Interface

To ensure that Communications Server can support NetMaster for TCP/IP you must authorize the interface between NetMaster for TCP/IP and your Communications Server environment.

### Task 1—Updating Your SOLVE SSI Configuration

To complete this task you must have write privileges for the NetMaster started tasks JCL.

NetMaster for TCP/IP uses the UNIX system services (USS) shell to issue the NETSTAT command. The interface to the USS shell is provided by a SOLVE SSI connected to your system and running on the same operating system image.

You can configure an existing SOLVE SSI to act as the USS interface, or you can create a new SOLVE SSI region.

To configure a SOLVE SSI, do this:

1. Access the SOLVE SSI started task JCL that you set up during your installation and setup procedure. See the *Unicenter Mainframe Installation and Setup Instructions* for more information.
2. To enable the NETSTAT interface, update your SOLVE SSI configuration to include the startup parameter UNIX=YES.
3. If you have multiple SOLVE SSIs configured in the same LPAR set XCF=YES in each SOLVE SSI. For example:

```
*-----  
*              SOLVE SSI INITIALIZATION PARAMETERS  
*-----  
SSID=QANM  
XEVNT=NO  
UNIX=YES  
XAPI=YES  
XCF=YES  
ENF=YES
```

## Task 2—Authorizing Your Started Task User IDs

**Important:** This task may have been done in the setup phase.

To complete this task you must have:

- Administration access to your security package
- OMVS shell write privileges

The sockets interface allows NetMaster for TCP/IP to perform TCP/IP related functions such as ping and traceroute.

The NETSTAT and sockets interfaces both require a USS security definition, referred to as an OMVS segment.

The TCP/IP started task user ID and the SOLVE SSI started task user ID:

- Can use a default OMVS segment
- Use a specific OMVS segment

To use your default OMVS segment, skip to Task 3, Authorizing User Functionality.

To set up an OMVS segment, do this:

1. Identify the NetMaster for TCP/IP started task user ID and the SOLVE SSI started task user ID that you want to authorize. These were set during installation. These can be the same user ID, or they can be different ones.
2. Choose an OMVS UID number to associate with each started task user ID. Your security administrator may have a policy for assigning OMVS UID numbers. If not, use a unique number.

For further information about OMVS UID numbers, see your IBM documentation.

3. Define the OMVS segment for the user. For a user ID *uuuuuuuu* and UID number *nnn*, do this:

For RACF systems enter:

```
ALU uuuuuuu OMVS(UID(nnn) HOME(/) PROGRAM(/bin/sh))
```

For CA-ACF2 systems enter:

```
SET PROFILE(USER) DIV(OMVS)  
INSERT uuuuuuu UID(nnn) HOME(/) PROGRAM(/bin/sh)
```

For CA-Top Secret systems enter:

```
TSS ADD(uuuuuuu) HOME(/) OMVSPGM(/bin/sh) UID(nnn)  
GROUP(OMVSGRP)
```

4. Ensure that you have completed this process for each started task user ID that you want to authorize. To confirm the contents of the OMVS segment, do this:

For RACF systems enter:  
LISTUSER *uuuuuu* OMVS NORACF

For CA-ACF2 systems enter:  
SET PROFILE(USER) DIV(OMVS)  
LIST *uuuuuu*

For CA-Top Secret systems enter:  
TSS LIS(*uuuuuu*) DATA(ALL)

4. Choose a home directory to associate with each started task user ID, and ensure that it exists and that the UID has at least read access to it.

You can use the UNIX root directory (/), or you can use a customized home directory name.

For example, to set up a directory called /u/name for UID*nnn* , issue the following commands in the OMVS UNIX shell:

```
mkdir /u/name  
chown nnn /u/name  
chmod 777 /u/name
```

5. Confirm the owner and access to the directory by using the command:

```
ls -l -d /u/solve
```

The result is displayed:

```
drwxrwxrwx  2 user  group 8192 Sep  31 14:58 /u/name
```



### Task 3—Authorizing User Functionality

NetMaster for TCP/IP uses OS/390 operator VARY commands to perform some functions. These include:

- Packet tracing
- Device activations and deactivations
- Dropping connections
- Verifying Telnet LU status

The user ID associated with NetMaster for TCP/IP must be authorized by your security system to issue these commands. The OPERCMDS resources to be accessed are:

- MVS.VARY.TCPIP.PKTTRACE
- MVS.VARY.TCPIP.OBEYFILE
- MVS.VARY.TCPIP.DROP
- MVS.VARY.TCPIP.TELNET.ACT
- MVS.VARY.TCPIP.TELNET.INACT

Authorize individual users to the OPERCMDS resources if you:

- Have configured your system to use SAF user security, for example by setting the startup parameter PPREF='SEC=PARTSAF' in your NetMaster for TCP/IP RUNSYSIN member
- Are using a partial security exit that returns SAF UTOKEN, for example NMSAFPX

For example, in a RACF system issue the command:

```
PE MVS.VARY.TCPIP.* CLASS(OPERCMDS) ID(uuuuuuu) ACCESS(UPDATE)
```

## Task 4—Enabling Access to SNMP Data

To complete this task you need write access to the Communication Server configuration datasets.

NetMaster for TCP/IP functions access information about Communications Server, using SNMP. For specific information about SNMP at your site see your TCP/IP administrator.

To enable these functions, do this:

1. Configure the SNMP agent (OSNMPD) by following the instructions in IBM's *Communications Server IP Configuration*.
2. Locate the PW.SRC dataset. This is typically in the SYSPWSRC DD statement. It can be:
  - An OS/390 dataset for example:  
//SYSPWSRC DD DISP=SHR,DSN=TCPIP.DATA(PWSRC)
  - In HFS file format, for example: /etc/pw.src
3. In the PW.SRC dataset configure a community name for use by the local host IP address .

**Important!** Community names are case-sensitive, the default community name is public in lower case.

Example—multiple IP addresses. If Communications Server has the IP addresses 192.168.8.1 and 192.168.1.2, then your PW.SRC dataset could contain something like:

```
public 192.168.0.0 255.255.0.0
```

Example—single IP address. If Communications Server has the IP addresses 192.168.0.1, then your PW.SRC dataset could contain something like:

```
public 192.168.0.0 255.255.255.255
```

It is not necessary to activate the SNMP Query Engine (SNMPQE), as the functions it performs are done internally by NetMaster for TCP/IP.

4. Locate the PROFILE dataset.
5. Set up the TCP/IP sub agent in the PROFILE dataset by following the instructions in IBM's *Communications Server IP Configuration*, for example:

```
SACONFIG COMMUNITY public AGENT 161  
SACONFIG ENABLED SETSENABLED
```
6. Activate the SNMP agent (OSNMPD) by following the instructions in IBM's *Communications Server IP Configuration*.

## Task 5—Ensuring That Name Resolution Is Enabled

Name lookup allows translation between IP addresses and host names. NetMaster for TCP/IP name lookup reads the TCPIP.DATA dataset and looks for the NSINTERADDR statements that contain the IP addresses of the name servers.

TCP/IP tries to resolve the host name through a name server, if one is configured in TCPIP.DATA. If the name cannot be resolved, the system uses the *prefix*.HOSTS.LOCAL dataset—this contains a list of names and addresses.

To ensure that name resolution is enabled, do this:

1. Locate the TCPIP.DATA dataset. This dataset is found in the JCL for the TCP/IP started task SYSTCPD DD statement. This can be:
  - A partitioned dataset member, for example:  
`//SYSTCPD DD DSN=TCPIP.DATA(DATAD1),DISP=SHR`
  - A sequential file, for example:  
`//SYSTCPD DD DSN=TCPIP.DATA,DISP=SHR`
2. Check that the TCPIP.DATA dataset is configured to suit your requirements.
3. Check that the *prefix*.HOSTS.LOCAL dataset is configured to suit your requirements.

For more information about the TCPIP.DATA and *prefix*.HOSTS.LOCAL datasets, see IBM's *OS/390 Communications Server IP Configuration*.

## Enabling Communications Server for Connection Awareness

Communications Server must be set up to generate the events and call the exits required for connection awareness of:

- Telnet events
- Connection events
- FTP events

### Task 1—Generating SMF Records

To complete this task you need access privileges to the Communications Server configuration DSNs.

The configuration members for Communications Server include parameters that:

- Specify which SMF records are created
- Identify the SMF subtypes

To set up SMF records creation, do this:

1. Check the PROFILE.TCPIP configuration member for TCP connect, FTP client, and Telnet client record creation.

The SMFCONFIG statement allows you to specify whether or not SMF records are created for:

- TCP connection start
- TCP connection end
- FTP and Telnet client records

For example:

```
SMFCONFIG TCPINIT TCPTERM FTPCLIENT TN3270CLIENT
```

An SMF record will not be created if you omit the SMFCONFIG statement or a particular parameter.

2. Check the PROFILE.TCPIP configuration member TELNETPARMS section for Telnet server record creation. The SMFINIT statement controls session start and the SMFTERM statement controls session end records.

For example:

```
TELNETPARMS
...
; Telnet Server connection SMF logging
SMFINIT STD
SMFTERM STD
ENDTELNETPARMS
;
```

The SMFINIT parameter sets the SMF record subtype for the Telnet server LOGN record. IBM have assigned a standard value of STD or 20 for this.

An SMF record will not be created if you omit these parameters or specify a value of zero.

3. Check the FTP.DATA configuration member FTP server records. It is recommended that you set SMF STD.

FTP server record creation is controlled by these SMF statements:

- SMF – all FTP server records
- SMFAPPE – FTP server append records
- SMFDEL – FTP server delete records
- SMFLOGN – FTP server logon failure records
- SMFREN – FTP server rename records
- SMFRETR – FTP server retrieve records
- SMFSTOR – FTP server store and store unique records

These records each specify the SMF record subtype value to be used for the specific events.

The SMF statement may be used to set the default value for all six types, for example:

```
SMF    STD
```

An SMF record will not be created if you omit these parameters.

4. If you have made any changes in step 3, restart the FTP server started task. If you have made any changes in steps 1 or 2, restart the TCP/IP started task.

## Task 2—Implementing the SMF Exit Module

To complete this task you need:

- SMF command privileges
- Write access to the SMF parameter datasets

An SMF exit module is provided in `?dsnpref.MS500.MSLOAD(NMSMFIBM)`.

1. Copy the NMSMFIBM executable module to a load library in the link list.
2. Issue an LLA refresh.

## Task 3—Registering the SMF Exit Module

To enable the SMF exits with OS/390 so that SMF can generate TCP connection records, FTP client records, and Telnet client records, register the SMF exits:

1. Access the SMFPRM`xx` member in SYS1.PARMLIB. Where `xx` is the SMF parameter member used in the IEASYS IPL configuration.
2. Check the SYS statement:
  - If TYPE is specified, ensure that TCP/IP record type 118 is included
  - If NOTYPE is specified, ensure that TCP/IP record type 118 is not included
    - Ensure that the exit names IEFU83, IEFU84, and IEFU85 are in the EXITS sublist

For example:

```
SYS (NOTYPE (16, 19, 64: 69) , EXITS (IEFU83, IEFU84, IEFU85, IEFACRT,
IEFUJV, IEFUSI, IEFUJI, IEFUTL, IEFU29) , INTERVAL (010000) , DETAIL)
```

3. If you have SUBSYS statements for the STC, TSO, or OMVS subsystems in the SMFPRM`xx` member, check the following:
  - If TYPE or NOTYPE is specified, ensure that TCP/IP record type 118 is processed
  - Ensure that the exit names IEFU83, IEFU84, and IEFU85 are in the EXITS sublist

4. If you have made any changes to your SMFPRM $xx$  member, restart SMF with the following command:

SET SMF= $xx$

where  $xx$  is the two-character member name suffix.

**Note:** You can enter the OS/390 commands from environments such as:

- SDSF
  - TSO option 6
  - NetMaster OCS or command entry using the SYSCMD command
5. For SMF to receive TCP connection, FTP, and Telnet records, activate your SMF exit module to OS/390.

OS/390 exit modules are registered using the EXIT ADD statement in a PROG $xx$  parameter of SYS1.PARMLIB. The PROG $xx$  is executed during an IPL. You can use the SET PROG= $xx$  command to add these after an IPL.

- a. To enable all the SMF exits to process on the next IPL, do this:
  - Locate the NMPROGCS sample update member provided as a source module in *?dsnpref*.MS500.INSTAL.
  - Copy the NMPROGCS member to SYS1.PARMLIB with the name PROG $xx$  (use your own values for  $xx$ ) and then follow the instructions that it contains. These describe how to make the necessary changes to the member and update the PROG $xx$  member for the next IPL
- b. To enable all the SMF exits immediately, do this:
  - Complete step a.
  - Use the SET PROG= $xx$  command to register the exit module immediately.
- c. To enable individual SMF exits, do this:
  - Use the SETPROG EXIT command. For example, to register module NMSMFIBM to the SYSSTC.IEFU84 exit name use the following command:

```
SETPROG EXIT,ADD,EXITNAME(SYS.IEFU84),MODNAME(NMSMFIBM)
```

## Task 4—Checking the MVS Dynamic Exits

The NetMaster for TCP/IP Self Test issues MVS commands to check the availability of an SMF exit. These commands relate to the MVS Dynamic Exits facility, which may be protected by your security system.

Ensure that your NetMaster for TCP/IP region has read access to the MVS Dynamic Exits facility. This is controlled by the general resource profile where:

- Class=FACILITY
- Profile=CSVDYNEX.LIST



# Preparing TCPaccess Systems

---

This chapter describes how to prepare TCPaccess so that it can work effectively with NetMaster for TCP/IP.

**This chapter contains the following topic:**

- Enabling the TCPaccess Interface

***Important:** Some of the tasks require high authority levels.*

## Enabling the TCPaccess Interface

Enabling the interface between NetMaster for TCP/IP and TCPaccess provides you with the authority to:

- Perform ping and traceroute functions
- Issue the NETSTAT and SYSSTAT commands
- Enable Connection Awareness

### Task 1—Setting Up the Parameter Datasets

1. If you have:
  - TCPaccess 5.2—apply either the SP0106 tape or the CUM0010 tape
  - TCPaccess 5.3—apply either the SP0106 tape or the CUM0102 tape
2. From the TCPaccess started task JCL locate the start configuration member.
3. Access the start configuration member and locate the TCPCFGxx statement to determine the TCPCFG member name.
4. Access the TCPCFG member and ensure that:
  - A RAW protocol statement is present—this statement enables the ping and traceroute functions.
  - A TCP protocol statement is present with MAXQLSTN specified to at least 25.

For example:

```
RAW MAXTSEND(9000) MAXTRECV(9000) MAXQSEND(8) MAXQRECV(8)
TCP PORTUSE(1:9999) PORTASGN(10000:20000)MAXQLSTN(25)
```

## Task 2—Enabling the TCPAccess Exit and Connection Awareness

For connection awareness, TCPAccess must:

- Have NMDSPAXS defined as an exit
- Be set up to generate the required SMF records

### Sub Task 2.1—Defining the TCPAccess Exit

To define the TCPAccess exit, do this:

1. Copy the NMDSPAXS load module supplied in *?dsnpref.MS500.MSLOAD* to a library accessible to TCPAccess, for example a library in the TCPAccess started task STEPLIB.
2. Open the IJTCFGxx configuration member.
3. Define NMDSPAXS as a TCPAccess exit by adding the following statement to the IJTCFGxx member:

```
EXIT PROGRAM (NMDSPAXS)
```

Insert the NMDSPAXS definition in the first position of the exit list. This ensures that the exit is always called.

## Sub Task 2.2—Generating SMF Records

To set up TCPAccess to generate SMF records, do this:

1. Access the IJTFCGxx configuration member. This is where the SMF record type and sub-types are specified.
2. Check that all of the subtypes that you require will be generated.

The SMF statement SUBTYPE parameter allows specific subtypes to be selected or suppressed. To generate subtypes, do this:

- If your SMF statement does not specify SUBTYPE – leave it as it is
- If the parameter is set to ALL – leave it as it is
- If the parameter is set to NONE – set it to ALL or a list of the subtypes that you require
- If the parameter is set to a list of subtypes – set it to ALL or a list of the subtypes that you require. The subtypes used by NetMaster for TCP/IP are:
  - SUBTYPE 20 – FTP dataset transfer completion (RETR, STOR, and APPE)
  - SUBTYPE 21 – FTP dataset modification (REN and DELE)
  - SUBTYPE 23 – Telnet server session termination
  - SUBTYPE 113 – TCP close

### Sub Task 2.3—Restarting TCPaccess

If you have changed your IJTFCGxx configuration member, do this.

1. Restart TCPaccess to bring the changes into effect.
2. Check the TCPaccess job log and the SYSLOG for the presence of these two messages:

```
T00EX004I NMDSPAXS: N6XA01 log message interface initialized
T00EX004I NMDSPAXS: N6XA02 Receiver ID $IPXssid will monitor messages from
TCPaccess
```

where *ssid* is the SSID of the TCPaccess job.

These messages are passed to your system during the TCPaccess initialization. Their presence indicates that the NetMaster for TCP/IP interface to TCPaccess has been set up correctly.

### Task 3—Setting Up DNR Members

To ensure that your TCPaccess Domain Name Resolver (DNR) members can translate the TCPaccess subsystem name into an IP address and a fully-qualified host name, do this:

1. Enable translation from subsystem name to fully-qualified domain name.

For example, if your TCPaccess subsystem name is ACSS and its fully-qualified domain name is MVS.SITE1.COM, enter a line like the following into your DNRALCxx member:

```
ACSS MVS.SITE1.COM.
```

Specify the domain name (rather than an IP address) and end it with a period (.).

2. Enable local translation of the fully-qualified host name to an IP address.

For example, if the IP address of MVS.SITE1.COM. is 123.12.123.112, enter a line like the following into your DNRHSTxx member:

```
MVS.SITE1.COM. 123.12.123.112
```

This DNR configuration is recommended in the *TCPaccess Customization Guide* that contains further details about the ACPCFGxx, TCPCFGxx, and DNRALCxx members of the TCPaccess parameter file.

3. Ensure that the HOSTTABLE statement in the DNRCFGxx member points to the correct DNRHSTxx member.
4. You do not need to restart TCPaccess to introduce changes to the DNR tables—you can restart DNR, for example:

```
F TCPICS,STOP DNR  
F TCPICS,START DNR
```

### Task 4—Enabling Access to SNMP Data

Some NetMaster for TCP/IP functions access information about TCPaccess, using SNMP.

To enable these functions, activate the SNMP Agent by updating the SNMCFGxx member in the TCPaccess PARM dataset. Make sure that you have a community value statement which includes the community name. The default community name is *public* in lower case.

See the *TCPaccess Customization Guide* for more information about updating the SNMCFGxx member.

## Task 5—Enabling the NETSTAT Interface

To enable the NETSTAT interface, do this:

Determine if your NetMaster for TCP/IP region has access to the TCPaccess LINK library. If it does not, add the TCPaccess LINK library to the STEBLIB concatenation in the JCL for your system.

See the *TCPaccess System Management Guide* for more information.





## Other Implementation Tasks

---

This chapter describes how to prepare your system for NetMaster for TCP/IP.

**This chapter contains the following topics:**

- Enabling the System Command Console Interface
- Setting Up OSA Support

## Enabling the System Command Console Interface

Some functions of NetMaster for TCP/IP involve the issuing of console commands and processing messages. To enable the monitoring of these functions, perform the following tasks.

### Task 1—Defining a Subsystem ID

To define a SubSystem ID (SSID), do this:

1. Add an SSID to IEFSSN $_{xx}$  in SYS1.PARMLIB. This becomes available when you next IPL.
2. Issue the following console command to make the SSID available immediately:  
`SETSSI ADD, SUBNAME=?SOLV`
3. Record the name of the SSID. You will need to specify it during the initial customization.

The console command interface SSID must be different to the SSID used by the SOLVSSI service task.

### Task 2—Defining Consoles

To define your consoles, do this:

1. Decide whether you are going to use extended MCS or JES consoles (extended MCS is recommended.)
2. If you are using JES consoles, you need to define them to MVS. Amend CONSOL $_{xx}$  in SYS1.PARMLIB to include the following statement for each JES console:  
`CONSOLE DEVNUM(SUBSYSTEM)`
3. You may need to IPL your system to activate the new JES consoles.

## Setting Up OSA Support

To enable OSA/SF functionality the OSA/SF load library must be available to your NetMaster for TCP/IP region. Examine the OS/390 linklist for SYS1.SIOALMOD. If SYS1.SIOALMOD is not in the linklist, do this:

1. Locate the started task JCL for the NetMaster for TCP/IP region.
2. Add SYS1.SIOALMOD to the STEPLIB DD statement in the started task JCL.

For example:

```
//STEPLIB DD DSN=dsnpref.MS500.MSLOAD,DISP=SHR
//          DD DSN=dsnpref.IP620.IPLOAD,DISP=SHR
//          DD DSN=SYS1.SIOALMOD,DISP=SHR
```

For full functionality, ensure that the following are in the same LPAR:

- The TCP/IP stack with the primary OSA device definition
- OSA/SF
- NetMaster for TCP/IP

The OSA/SF API task is required to:

- Monitor OSA performance
- Issue configuration actions against OSA resources



# Initializing NetMaster for TCP/IP

---

This chapter describes how to initialize the region.

**This chapter contains the following topics:**

- Initializing NetMaster for TCP/IP for the First Time
- Dealing with Initialization Failures

## Initializing NetMaster for TCP/IP for the First Time

Perform the following tasks to get your NetMaster for TCP/IP system running.

### Task 1—Logging On

1. Ensure that the NetMaster for TCP/IP region has started and the primary ACB has opened.
2. Enter LOGON APPLID(acb-name), using the ACB name of the NetMaster for TCP/IP region. The logon panel is displayed.
3. Enter the user ID and password. You are prompted to change your password.
4. Press F3 (File) to change your password. After your password is changed, the initial System Parameters Customization panel is displayed.

### Task 2—Performing Initial Customization

Various installation-specific parameters must be set using Initialization and Customization Services (ICS).

Customization can only be performed by a user with UAMS maintenance authority. That user's UAMS definition should have an APPC Access Key value of ALL, if a value is not already specified.

## Initialization Setup Types

From the initialization dialog panel, you can select:

- **Fast Setup**—this option enables you to review and customize only required parameter groups. It is used to implement your region as quickly as possible. It provides default values wherever possible, but enables you to review all the required parameter groups to ensure that they match your installation standards. You can customize other parameters at a later date.
- **Custom Setup**—this option enables you to review and customize the required parameter groups and additional file and dataset names, to bring the system operation closer to your installation standards. It is used to implement your region quickly, while still performing some initial customization. This option provides some default values, enables you to specify names for certain files and datasets, and enables you to review the required parameter groups (these are flagged).
- **Complete Setup**—this option enables you to review and customize all initialization and customization parameters.

## Customizing Parameter Values

All parameters have default values. To customize parameter values, do this:

- To review a parameter group, enter U beside it.
- Make any changes that you require.
- Press F6 (Action) to action the change immediately.
- Press F3 (File) to save your changes and indicate that you have reviewed the group.
- If you need assistance, press F1 to get online help.

The value you assign to a parameter is associated with the performance of one or more actions, such as setting SYSPARMS or allocating datasets. You can action some parameter groups as soon as you enter appropriate values on the parameter panel. When, however, you change the value of parameters such as the system ID or MODS file names, these parameter values can only be actioned by restarting the NetMaster for TCP/IP region.

## Exiting Before Completing Customization

If you attempt to exit the customization process before reviewing all required parameter groups, you are presented with a confirmation screen. You can choose to log off and continue with the customization later. Alternatively, another user can log on at a later time and complete the customization process. Users cannot access the region until all the required parameter groups have been reviewed.

## Sub Task 2.1—Updating and Reviewing the Fast Setup Customization Parameters

Select the Fast Setup Customization Parameters option. The ICS : Fast Setup Customization panel is displayed.

```

PROD----- ICS : Fast Setup Customization -----5
Command ==>                                     Scroll ==> PAGE

                S/B=Browse U=Update/Review H=Help L=ILog SD=Set Default
Review each of the following parameter groups to ensure that they meet your
installation's standards.

Reviewed?  Short Description                Required?  Parameter Group ID
External Applications Access                YES       $RM  EXTAPPLS
Links to NetSpy systems                    YES       $ES  NETSPYLINKS
Operating System Identifiers               YES       $RM  OPSYSIDS
System Identifications                    YES       $NM  SYSTEMID
SOLVE Sub-System Interface                 YES       $NM  SSI
TCP/IP Sockets Interface                  YES       $NM  SOCKETS

**END**

F1=Help      F2=Split    F3=Exit          F5=Find      F6=Refresh
F7=Backward  F8=Forward   F9=Swap        F11=Right
  
```

The EXTAPPLS and NETSPYLINKS parameter groups are only displayed if you have Unicenter NetSpy Network Performance. The SSI parameter group is not displayed if the SSID parameter is defined in your RUNSYSIN member.



### Sub Task 2.2—Implementing External Applications Access

1. Enter **U** beside the External Applications Access parameter group. The EXTAPPLS - External Applications Access panel is displayed.
2. Enter the NetSpy SNA Agent Application Specification Application Name.
3. For information on the remaining fields press F1 (Help.)
4. Press F6 (Action) to action the entries.
5. Press F3 (File) to save your settings. The Fast Setup Customization Panel appears with the External Applications Access Reviewed field marked as YES.

### Task 2.2—Implementing Links to NetSpy Systems

1. Enter **U** beside the Links to NetSpy Systems parameter group. The NETSPYLINKS - Links to NetSpy SNA Agents panel is displayed.
2. Enter the NetSpy NSYXname ACB Name. This is used for:
  - NetSpy SNA Agent to NetSpy communication
  - NetSpy SNA Agent to NetMaster for TCP/IP communication
3. For information on the remaining fields press F1(Help.)
4. Press F6 (Action) to action the entries.
5. Press F3 (File) to save your settings. The Fast Setup Customization Panel appears with the Links to NetSpy Systems Reviewed field marked as YES.

### Sub Task 2.3—Implementing Operating System Identifiers Parameters

1. Enter **U** beside the OPSYSIDS parameter group. The OPSYSIDS - Operating System Identifiers panel is displayed.
2. Complete the fields on this panel.
  - Ensure that the AOM subsystem ID is the same as that assigned in the SYS1.PARMLIB(IEFSSNxx) dataset member during setup. AOM is a subsystem interface that enables system message flow to the region.
  - If you use command characters for other tasks, ensure that the command characters in this parameter group are not in conflict with them.
  - If the system uses the JES3 job entry subsystem, ensure that information about the job entry subsystem is updated
  - Press F1 (Help) for more information.
3. Press F6 (Action) to action the entries.
4. Press F3 (File) to save your settings. The Fast Setup Customization Panel appears with the Operating System Identifiers Reviewed field marked as YES.

### Sub Task 2.4—Implementing System Identifications Parameters

1. Enter **U** beside the System Identifications parameter group. The SYSTEMID - System Identifications panel is displayed.
2. If required, you can change the:
  - System ID
  - Logon Panel Title
  - OCS Title
3. Press F6 (Action) to action the entries.
4. Press F3 (File) to save your settings. The Fast Setup Customization Panel is displayed with the System Identifications Reviewed field marked as YES.

### Sub Task 2.5—Implementing SSI - SOLVE Sub-System Interface Parameters

1. Enter **U** beside the SSI parameter group. The SSI - SOLVE Sub-System Interface panel is displayed.
2. Complete the fields on the panel. By default, this parameter group uses the subsystem interface (SSI) ID specified by the SSID parameter of a PPREF statement in your RUNSYSIN member. This is the ID assigned to the SOLVE SSI service task during setup.

For more information press F1(Help) .

3. Press F6 (Action) to action the entries.
4. Press F3 (File) to save your settings. The Fast Setup Customization Panel is displayed with the SOLVE Sub-System Interface Reviewed field marked as YES.

### Sub Task 2.6—Implementing the TCP/IP Sockets Interface Parameters

1. Enter **U** beside the TCP/IP Sockets Interface parameter group. The SOCKETS - TCP/IP Sockets Interface panel is displayed.
2. Tab to the TCP/IP Software Type input field, and enter the required value. Only one type of TCP/IP software can be configured as the sockets interface in each region.
3. Complete the fields on the panel. For information on the fields press F1 (Help).
4. Press F8. The second panel for this parameter group is displayed.
5. Complete the fields on the panel. For information on the fields press F1 (Help).
6. When you have completed all the fields, press F6 (Action) to set the specified values and start the interface.
7. Press F3 (File) to save your settings. The Fast Setup Customization Panel appears with the TCP/IP Sockets Interface Reviewed field marked as YES.
8. Press F3 (Exit). The ICS : System Parameters Customization panel is displayed.

### Task 3—Reviewing Additional Parameter Groups

Depending on which product features you want to implement, you might need to review other parameter groups. You can review these parameter groups:

- Now — select the Complete Setup Customization Parameters option to list all parameter groups and review the relevant groups. When you complete the review, exit the list and the System Parameters Customization panel.
- Later — exit the System Parameters Customization panel. (When you are ready to review these parameter groups, enter the **=/ICS** shortcut to list the groups.)

### Task 4—Express Setup

The express setup discovers your system's IP resources and stores their definitions in a system image. Express setup starts automatically during your first log in.

Express setup relies on SNMP and NETSTAT enablement. Ensure that these are correctly configured for the stack configured *Sub Task 2.6 – Implementing the TCP/IP Sockets Interface Parameters*.

To run the express setup, do this:

1. Exit from the System Parameters Customization panel. The Automation Services : Confirm Express Setup panel is displayed.

```

PROD----- Automation Services : Confirm Express Setup -----
Command ==>

                                EXPRESS SETUP

This facility will automatically find your installation's resources and
define them in the database.

The discovered resources are placed in a newly created System Image.
The Control Member defines which resources are to be discovered.

You can elect to have the system image loaded as the 'active image' when
Express Setup has completed by typing YES next to Load Image?.

Express Setup will use the following parameters:
System Image ..... SAMP
Version ..... 0001
Control Member ..... $RMEXPR6
Load Image? ..... NO

Press the Action key to confirm the request or the Exit key to cancel
F1=Help      F2=Split      F3=Exit      F6=Action
              F9=Swap
    
```

2. Specify values in the System Image and Version fields. These default to the local OS/390 system name and version 0001 for the first time administration process.
3. The \$RMEXPR6 Control Member defaults to discover all of your IP resources. To configure the \$RMEXPR6 control member, do this:
  - a. Copy \$RMEXPR6 into TESTEXEC.
  - b. Update the \$RMEXPR6 TESTEXEC member to your site's specifications. (For example, comment out the resources you do not need to discover.)
  - c. Rename \$RMEXPR6 and use this in the Control Member field.
4. To load this system image after the discovery has completed set Load Image? to YES.

**Note:** To permanently load this system image on future NetMaster for TCP/IP restarts update the /ICS AUTOIDS parameter group. For more information see Task 5 – Setting up the System Image to Load on Restart.

5. Press F6=Action. The Automation Services : Express Setup Status panel is displayed. This panel reports the progress of the IP resource discovery and the number of resources successfully discovered. The time taken to complete this process is determined by your site's IP configuration.

See the *NetMaster for TCP/IP Administration Guide* for information on reviewing and administering the IP resources discovered by the express setup.

**Tip:** To access express setup after your first log on, enter /RADMIN.AD.I at the ==> prompt

## Task 5—Setting up the System Image to Load on Restart

To ensure that the system image built by express setup is loaded during initialization, do this:

1. Entering **/ICS** at the **==>** prompt. The ICS : Customization Parameters panel is displayed.
2. Select the AUTOIDS parameter group in update mode. The ICS : Initialization Parameters panel is displayed.

```

PROD----- ICS : Initialization Parameters -----Page 1 of 1
Command ==>                                         Function=Update

  AUTOIDS - Automation Identifiers

System Image Name (1) .....+ ?
Version (1) .....+
Automation Mode (1) ..... MANUAL      (Automated or Manual)
Default Desired State ..... ACTIVE    (Active or Inactive)
Perform Action in Manual Mode? ..... NO (Yes or No)

Checkpoint Restart Status ..... ACTIVE (Active or Inactive)
Cold Start on Next Restart? (1) .... NO (Yes or No)

Confirm via WTOR at Startup? ..... NO  (No,Yes,seconds to confirm
                                         parameters denoted by (1) )

Role in Multi-system Operation ..... FOCAL

Notes N
Warning: If actioned the specified System Image will be reloaded.

F1=Help      F2=Split      F3=File      F4=Save      F5=ILog      F6=Action
              F9=Swap                                F12=Cancel
  
```

3. Enter **?** in the System Image Name field. The ResourceView : System Image List panel is displayed.
4. Select the System Image and Version you specified during the Express Setup.
5. Press **F6=Action** if the system image is not already loaded.

**Important!** *F6=Action replaces the currently loaded system image. If you do not want to load the system image now, skip this step.*

6. Press **F3=File**. The system image will load each time the NetMaster for TCP/IP region starts.

## Task 6—Changing User to Administrator

Before you log off, change the initial user to an administrator by using the \$RMADMIN group definition as a model.

1. Enter **/ASADMIN.UP** to display the User Profile List panel.
2. Press F4 (Add) to add a new user profile. The action presents you with the first panel in the user profile definition, the User Description panel.
3. Enter the ID of the initial user. The panel is refreshed with the existing information about the user.
4. Enter **\$RMADMIN** in the Group ID field to give the user administrative authority.
5. Press F3 (File) to save the record.

## Dealing with Initialization Failures

If you log on to a region that has failed any initialization parameter groups, ICS displays the System Initialization In Progress dialog to indicate progress, and to assist you in identifying and rectifying any problems.

Fatal errors occur (for example, you are unable to log on) if either or both of the following are unavailable:

- Panel libraries
- MODS control files

### Using the System Initialization In Progress Dialog

The System Initialization In Progress dialog shows you the current initialization status and whether actions associated with parameter groups have failed.

If a failure occurs:

- Press F8 to scroll to the bottom of the System Initialization in Progress panel.
- Enter S next to failed parameters
- View the log for the failed group – look for error messages
- Use the message help and the full activity log to determine the cause of the failure
- Make the necessary changes to the parameter group
- Action the parameter group



## Parameter Group Actions

You can apply the following actions to listed parameter groups:

- **S** or **B** (Browse) to browse parameter group details
- **H** (Help) to view help for a parameter group
- **U** (Update) to update parameter group details
- **AC** (Action) to action a parameter group
- **L** (ILog) to view the associated initialization and customization log
- **I** (Ignore) to indicate to the system that it should ignore a failed parameter group, and proceed to run dependent parameter groups

See the online help for additional assistance.

An action can only be performed against an already completed parameter group or a failed parameter group.

Ignoring parameter groups is not recommended; consider carefully before applying this action.

When you correct an error by updating an incorrect parameter group record, you have to action that parameter group before processing can continue (unless you apply the Ignore action). Action the parameter group in one of the following ways:

- By pressing F6 (the Action key) when you finish updating the parameter group
- By applying AC (Action) to the listed parameter group

## Where to Next?

You have now completed the implementation tasks. To set up NetMaster for TCP/IP, follow the instructions in the *NetMaster for TCP/IP Administrator Guide*.